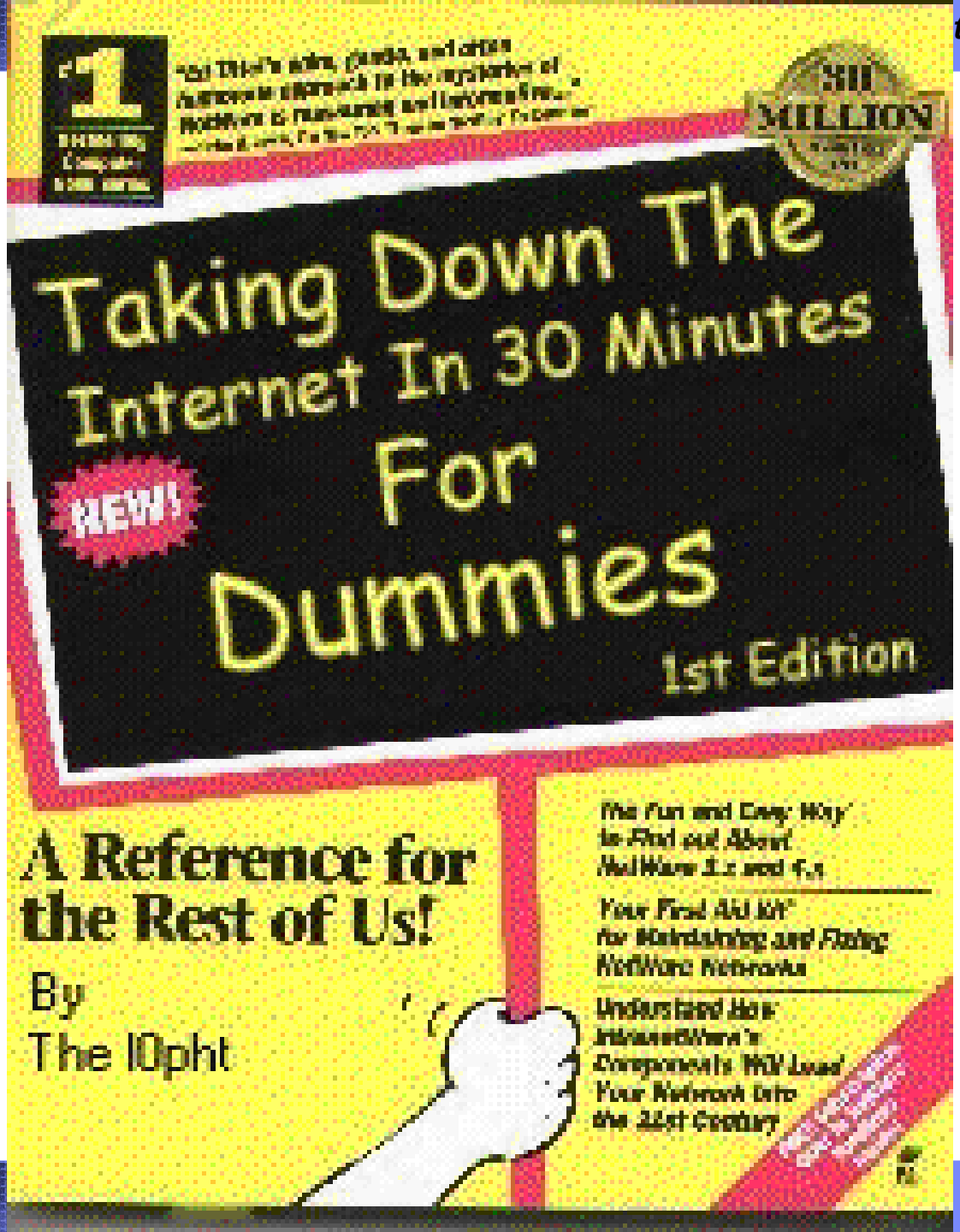


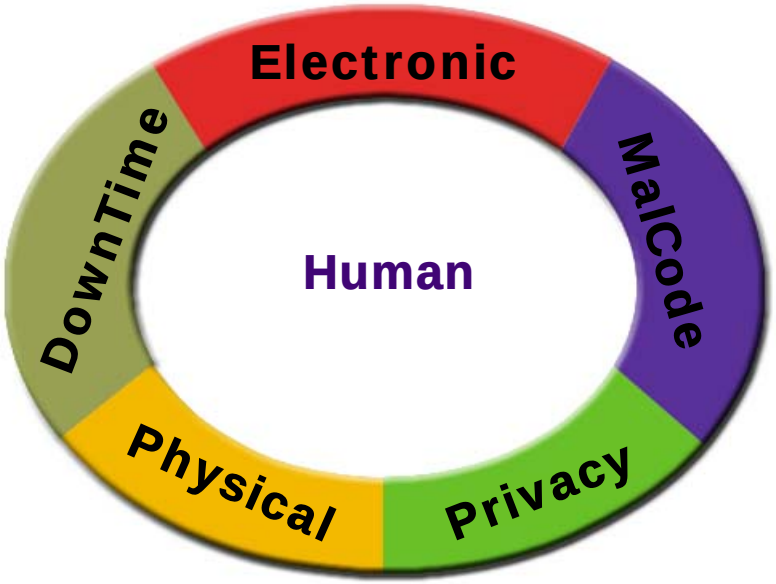
The Fine Line

From Wikipedia:

- **Risk Assessment:** Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat.
- **Vulnerability Assessment:** A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- **Security Audit**: A computer security audit is a manual or systematic measurable technical assessment of a network, system or application.
- **Penetration Testing:** is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user… The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

Six Categories of Risk

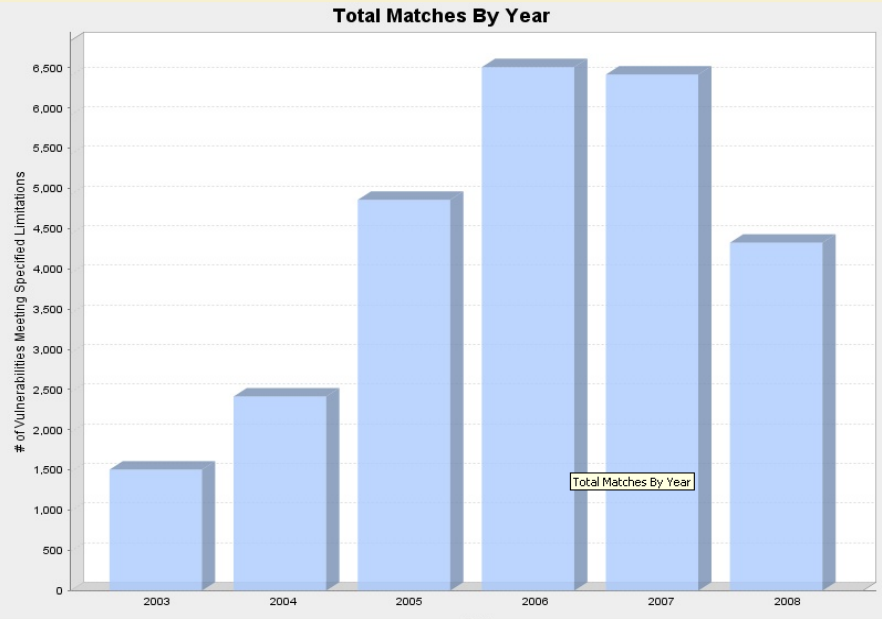
- Electronic
  - (External / Internal)
  - Hacking, Sniffing
  - Spoofing
- Malicious Code
  - Viruses, Worms
  - Java, ActiveX
  - Trojans
- Physical
  - Theft, Terminal hijack
- Human
  - Social Engineering
  - Bad Eggs, Sticky-note
- Privacy
  - employee
  - customer data
  - corporate data
- DownTime
  - DoS attacks
  - Bugs
  - Power
  - Civil Unrest
  - Natural Disasters

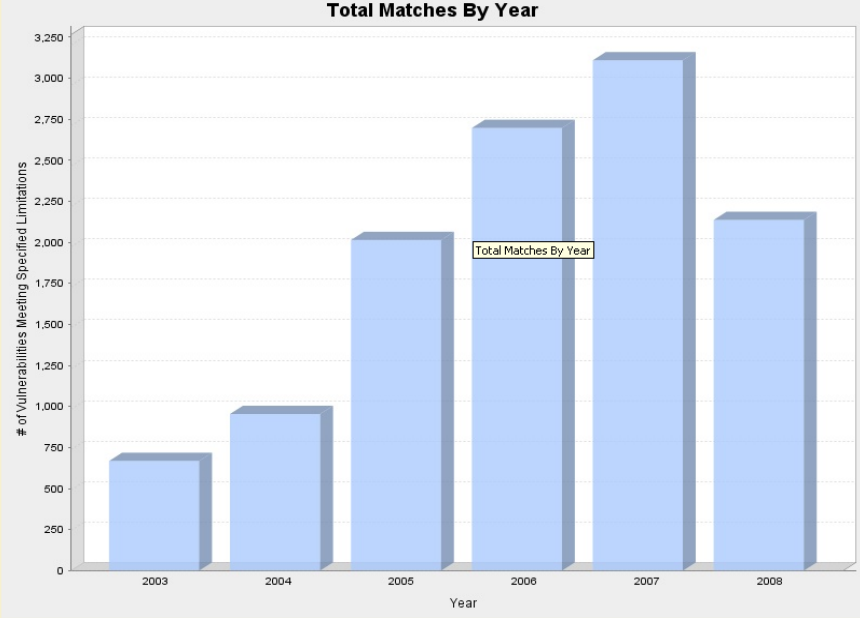


Impact of Vulnerabilities

average annual loss reported by U.S. companies in the 2007 CSI Computer Crime and Security Survey more than doubled, from $168,000 in last year's report to $350,424 in this year's survey [newmedia.org]

Number of reported vulnerabilities each year is increasing [CERT stats]





Source: ©2002-2008 The SANS™ Institute, http://www.sans.org/top20/

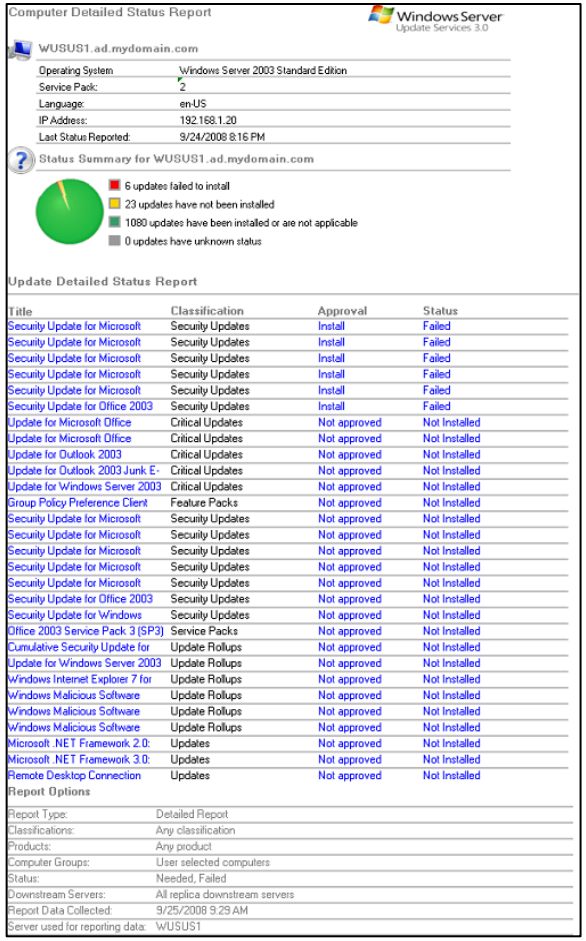
SANS Top 20 Vulnerabilities - ***UPDATE***

NEW

- **Windows**
  - W1. Windows Services
  - W2. Internet Explorer
  - W3. Windows Libraries
  - W4. Microsoft Office and Outlook Express
  - W5. Windows Configuration Weaknesses
- **Networking**
  - N1. Cisco IOS and non-IOS Products
  - N2. Juniper, CheckPoint and Symantec Products
  - N3. Cisco Devices Configuration Weaknesses
- **UNIX**
  - U1. UNIX Configuration Weaknesses
  - U2. Mac OS X
- **Cross-Platform**
  - C1. Backup Software
  - C2. Anti-virus Software
  - C3. PHP-based Applications
  - C4. Database Software
  - C5. File Sharing Applications
  - C6. DNS Software
  - C7. Media Players
  - C8. Instant Messaging Applications
  - C9. Mozilla and Firefox Browsers
  - C10. Other Cross-platform Applications

What To Assess??

Traditionally....



Computer Detailed Status Report

Windows Server Update Services 3.0

WUSUS1.ad.mydomain.com

Operating System:	Windows Server 2003 Standard Edition
Service Pack:	2
Language:	en-US
IP Address:	192.168.1.20
Last Status Reported:	9/24/2008 8:16 PM

Status Summary for WUSUS1.ad.mydomain.com

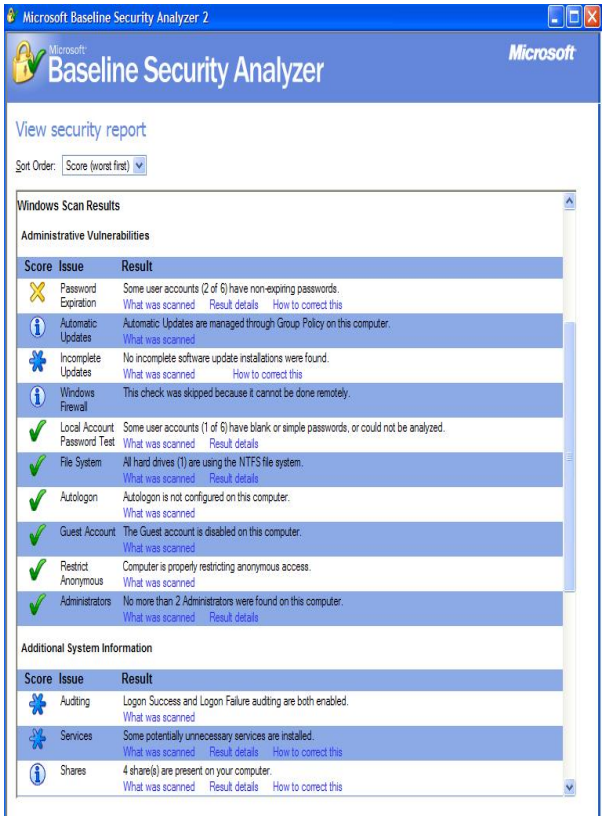
6 updates failed to install
23 updates have not been installed
1080 updates have been installed or are not applicable
0 updates have unknown status

Update Detailed Status Report

Title	Classification	Approval	Status
Security Update for Microsoft	Security Updates	Install	Failed
Security Update for Microsoft	Security Updates	Install	Failed
Security Update for Microsoft	Security Updates	Install	Failed
Security Update for Microsoft	Security Updates	Install	Failed
Security Update for Microsoft	Security Updates	Install	Failed
Security Update for Office 2003	Security Updates	Install	Failed
Update for Microsoft Office	Critical Updates	Not approved	Not Installed
Update for Microsoft Office	Critical Updates	Not approved	Not Installed
Update for Outlook 2003	Critical Updates	Not approved	Not Installed
Update for Outlook 2003 Junk E-	Critical Updates	Not approved	Not Installed
Update for Windows Server 2003	Critical Updates	Not approved	Not Installed
Group Policy Preference Client	Feature Packs	Not approved	Not Installed
Security Update for Microsoft	Security Updates	Not approved	Not Installed
Security Update for Microsoft	Security Updates	Not approved	Not Installed
Security Update for Microsoft	Security Updates	Not approved	Not Installed
Security Update for Microsoft	Security Updates	Not approved	Not Installed
Security Update for Microsoft	Security Updates	Not approved	Not Installed
Security Update for Office 2003	Security Updates	Not approved	Not Installed
Security Update for Windows	Security Updates	Not approved	Not Installed
Office 2003 Service Pack 3 (SP3)	Service Packs	Not approved	Not Installed
Cumulative Security Update for	Update Rollups	Not approved	Not Installed
Update for Windows Server 2003	Update Rollups	Not approved	Not Installed
Windows Internet Explorer 7 for	Update Rollups	Not approved	Not Installed
Windows Malicious Software	Update Rollups	Not approved	Not Installed
Windows Malicious Software	Update Rollups	Not approved	Not Installed
Windows Malicious Software	Update Rollups	Not approved	Not Installed
Microsoft .NET Framework 2.0:	Updates	Not approved	Not Installed
Microsoft .NET Framework 3.0:	Updates	Not approved	Not Installed
Remote Desktop Connection	Updates	Not approved	Not Installed

Report Options

Report Type:	Detailed Report
Classifications:	Any classification
Products:	Any product
Computer Groups:	User selected computers
Status:	Needed, Failed
Downstream Servers:	All replica downstream servers
Report Data Collected:	9/25/2008 9:29 AM
Server used for reporting data:	WUSUS1



Microsoft Baseline Security Analyzer 2

Microsoft Baseline Security Analyzer

Microsoft

View security report

Sort Order: Score (worst first)

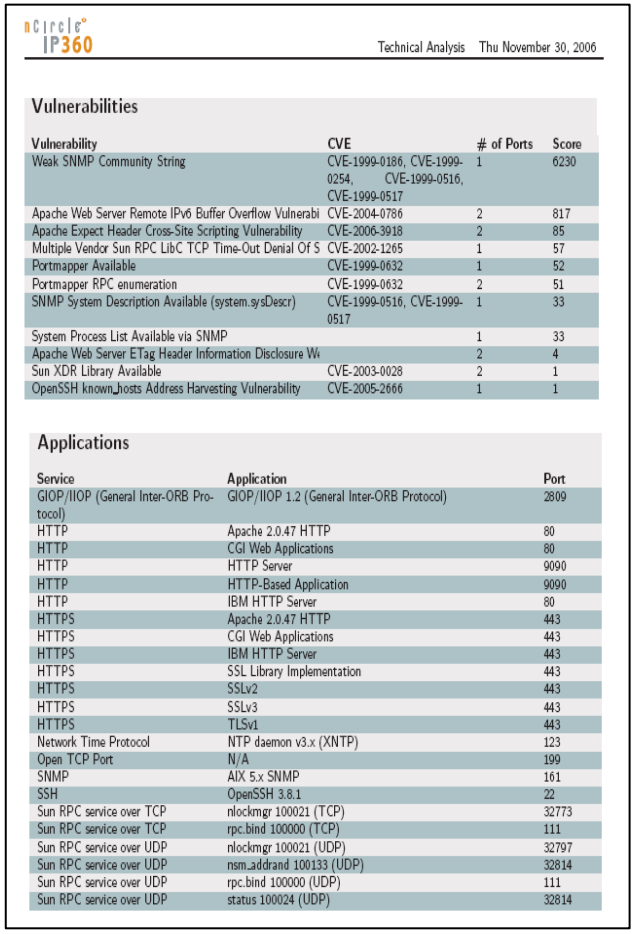
Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Password Expiration	Some user accounts (2 of 6) have non-expiring passwords. What was scanned Result details How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
	Incomplete Updates	No incomplete software update installations were found. What was scanned How to correct this
	Windows Firewall	This check was skipped because it cannot be done remotely.
	Local Account Password Test	Some user accounts (1 of 6) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details

Additional System Information

Score	Issue	Result
	Auditing	Logon Success and Logon Failure auditing are both enabled. What was scanned
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	4 share(s) are present on your computer. What was scanned Result details How to correct this



nCircle IP360

Technical Analysis Thu November 30, 2006

Vulnerabilities

Vulnerability	CVE	# of Ports	Score
Weak SNMP Community String	CVE-1999-0186, CVE-1999-0254, CVE-1999-0516, CVE-1999-0517	1	6230
Apache Web Server Remote IPv6 Buffer Overflow Vulnerabi	CVE-2004-0786	2	817
Apache Expect Header Cross-Site Scripting Vulnerability	CVE-2006-3918	2	85
Multiple Vendor Sun RPC LibC TCP Time-Out Denial Of S	CVE-2002-1265	1	57
Portmapper Available	CVE-1999-0632	1	52
Portmapper RPC enumeration	CVE-1999-0632	2	51
SNMP System Description Available (system.sysDescr)	CVE-1999-0516, CVE-1999-0517	1	33
System Process List Available via SNMP		1	33
Apache Web Server ETag Header Information Disclosure W		2	4
Sun XDR Library Available	CVE-2003-0028	2	1
OpenSSH known_hosts Address Harvesting Vulnerability	CVE-2005-2666	1	1

Applications

Service	Application	Port
GIOP/IIOP (General Inter-ORB Protocol)	GIOP/IIOP 1.2 (General Inter-ORB Protocol)	2809
HTTP	Apache 2.0.47 HTTP	80
HTTP	CGI Web Applications	80
HTTP	HTTP Server	9090
HTTP	HTTP-Based Application	9090
HTTP	IBM HTTP Server	80
HTTPS	Apache 2.0.47 HTTP	443
HTTPS	CGI Web Applications	443
HTTPS	IBM HTTP Server	443
HTTPS	SSL Library Implementation	443
HTTPS	SSLv2	443
HTTPS	SSLv3	443
HTTPS	TLSv1	443
Network Time Protocol	NTP daemon v3.x (XNTP)	123
Open TCP Port	N/A	199
SNMP	AIX 5.x SNMP	161
SSH	OpenSSH 3.8.1	22
Sun RPC service over TCP	nlockmgr 100021 (TCP)	32773
Sun RPC service over TCP	rpc.bind 100000 (TCP)	111
Sun RPC service over UDP	nlockmgr 100021 (UDP)	32797
Sun RPC service over UDP	nsm_addrand 100133 (UDP)	32814
Sun RPC service over UDP	rpc.bind 100000 (UDP)	111
Sun RPC service over UDP	status 100024 (UDP)	32814

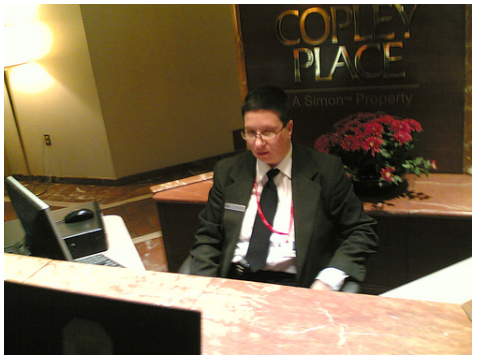
We worry about…

But, have we considered...

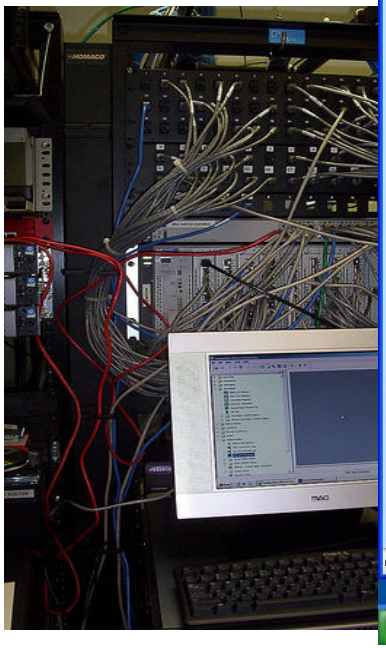
Click Here

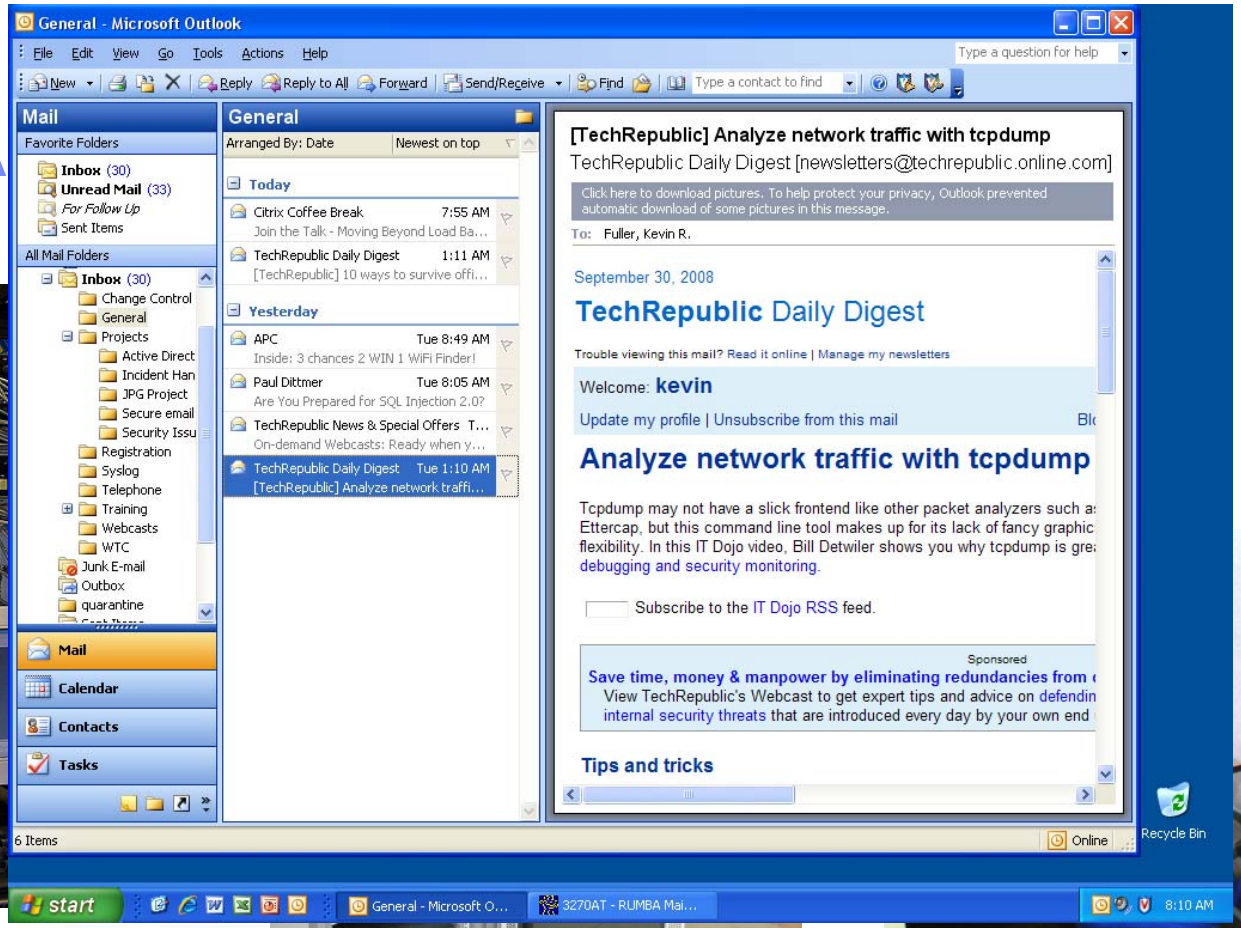
What about Software….

What About……

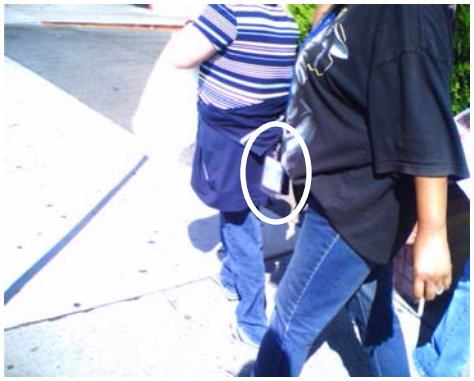


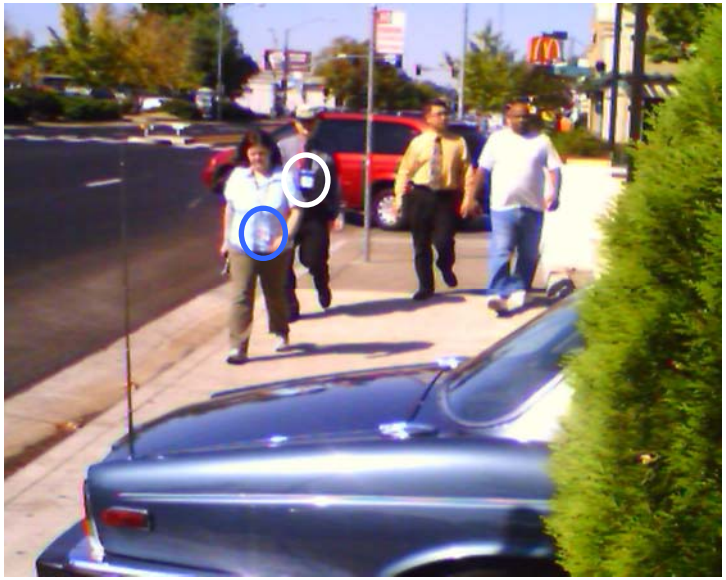
OR How A





Where is the Risk Here??





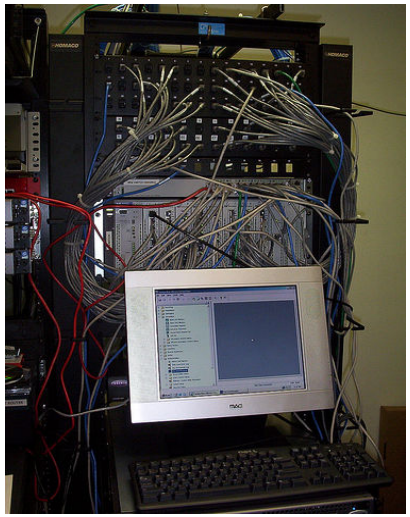
Have you considered…..

Why???...

What would happen if…

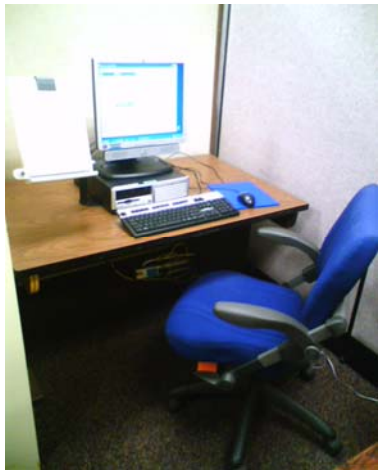
OR

With

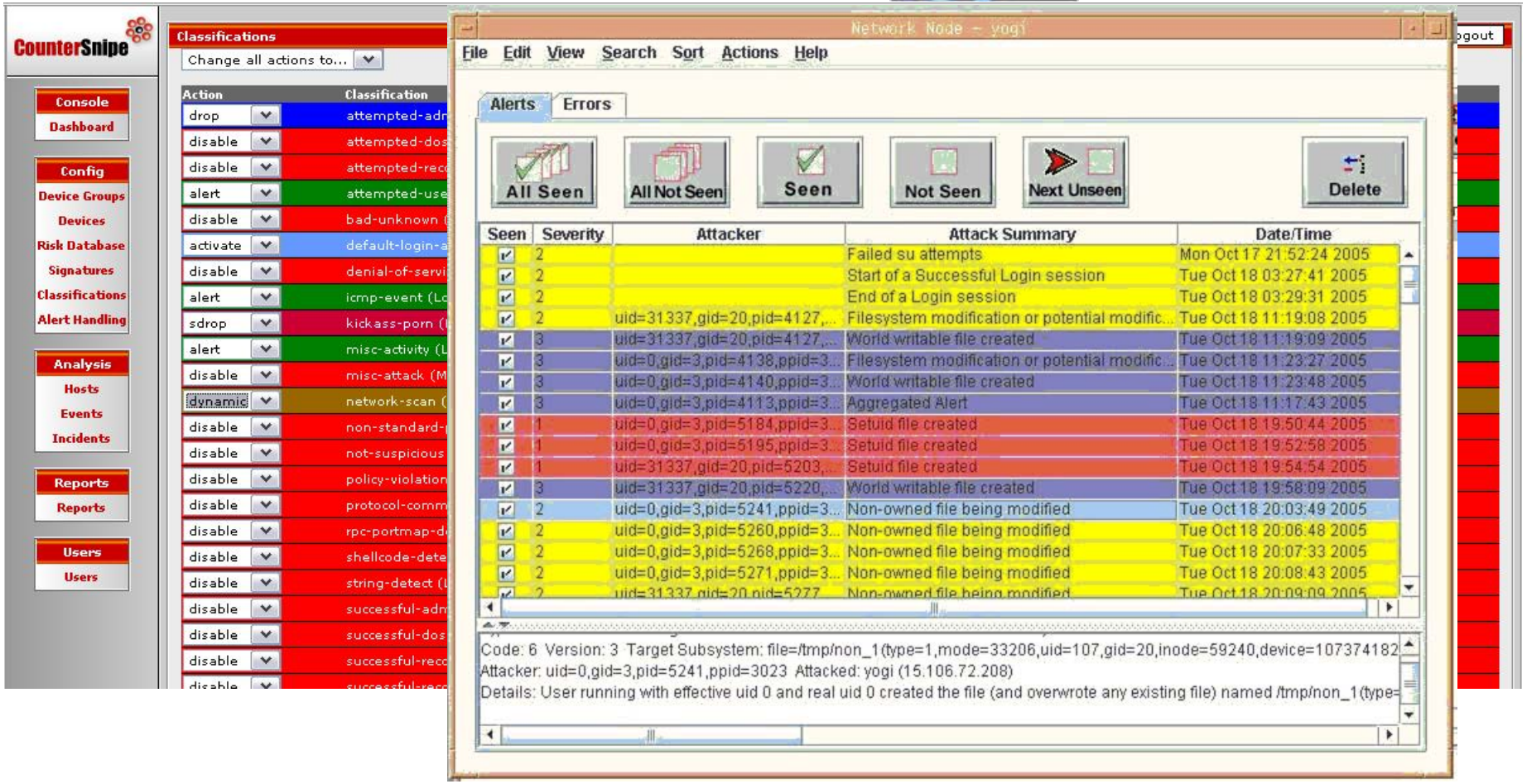


AND

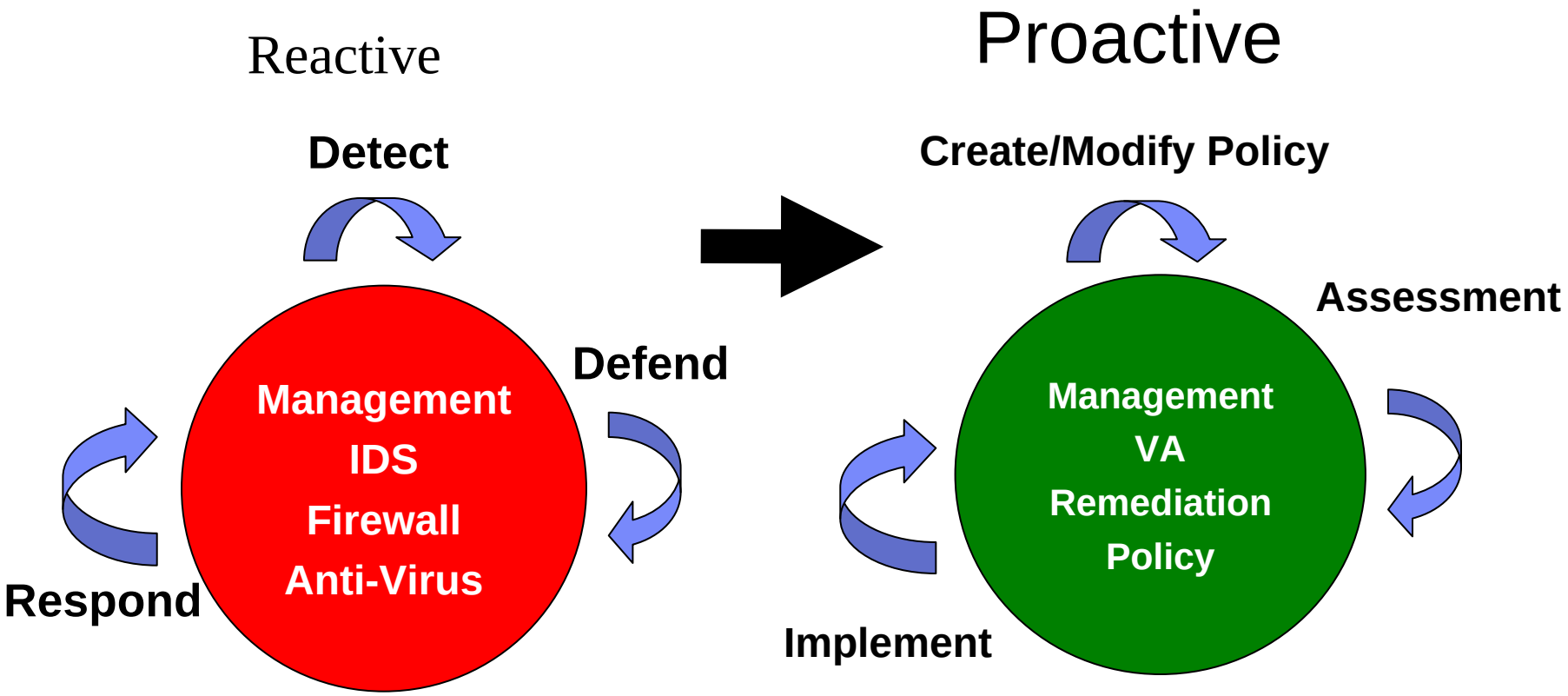
With



The result could be…..



Industry Direction: Proactive



Vulnerability Assessment: What's the Value??

1. Add Value to Risk

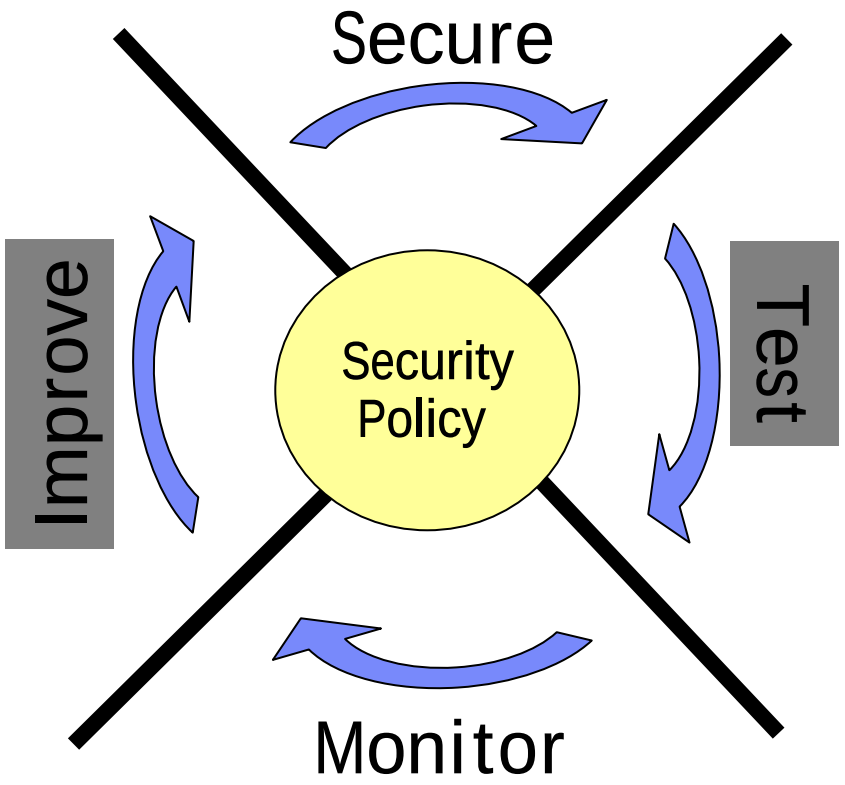
- A CIO could run a complete scan in a matter of hours with a VA product.
  - This to determine the critical issues
  - Quarantine / Scrubbing of suspicious IP devices
- Analysis can yield huge amounts of data, but a good VA tool will
  - Automatically generate a report
  - Prioritize data
  - Allow decisions to be made on actions
- Once a baseline is established, segment the network into areas of criticality.

2. Assessing Vulnerabilities

- Get a "hacker's eye view" of network
- Once you get a report, establish reporting processes.
- Conduct regression testing
- Check for any vulnerability issues that might have arisen from updates.

Continuous Network Security

- **Security Testing Is essential**
  - Develop policies
  - Build security infrastructure
  - Establish security baseline
  - Assess risks
  - Identify threats and vulnérabilités
  - Remediate
  - Assess again…
  - Revisit Security Policy



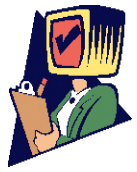
How to Assess Vulnerabilities

- **Low Tech**
  - Review Policy
  - Interview
  - Document Review
  - Review in Action
- **High Tech**
  - Use Vulnerability Scanning Tools

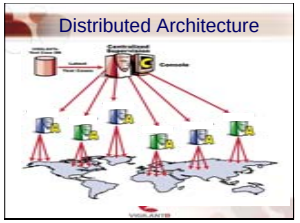
Vulnerability Scanner Evolution

- **1st Generation: Hacker's tools**
  - **Mostly open source, underground: Cheops, NMAP, Satan…**

- **2nd Generation: Automatization of hacker's tools**
  - **Focus on scripted attacks: Test Cases**
    - **Packages: ISS, NAI, Nessus, Symantec …**
    - **ASP's: Qualys, Foundstone, Intranode**
  - **Deployment and performance issues (point-in-time, segment-based, unrelated reports)**



- **3rd Generation: Network-based scanners, infrastructure testing heritage**
  - **Focus on distributed architecture: centralized supervision of global network security testing**
  - **Live update of vulnerability signatures**
  - **Automation**



Vulnerability Scanners

- Categories
  - Software
    - Open Source: Saint, SCAP
    - Commercial/Closed Source: ISS, Nessus
  - Appliance: NCircle
  - Software as a Service: Qualys
- Types

  General

  Web based
  - Code Analysis: DevInspect,
  - Web Site/Application Analysis: WebInspect, ...App Detective

A real smorgasbord of products!!!

How do Vulnerability Scanners work???

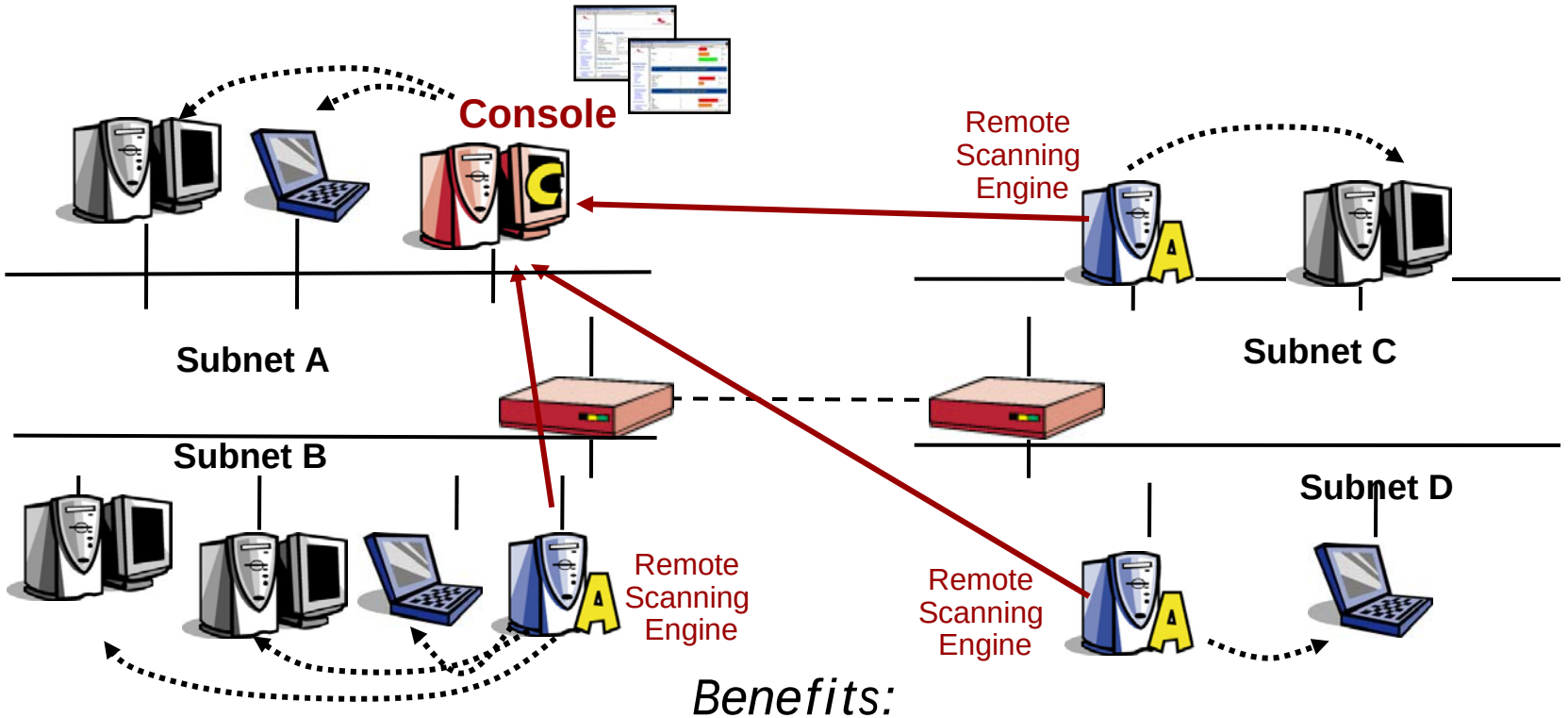
- **They utilize:**
  - Known repositories of vulnerabilities
    - Open Source Vulnerability Database (OVDB)
    - Common Vulnerability Exposures (CVE)
    - National Vulnerability Database (NVD)
  - Known information on vender patches
  - Results from security research
- **They look for**:
  - Version information/date stamps on particular files and folders
  - Presence of vulnerable code syntax in files and applications
  - Open TCP/IP Ports
  - Configuration settings
  - Registry settings (Windows)
  - ????
- **Their output:**
  - Report on scan targets
  - Identified vulnerabilities
  - Generic risk rating based on severity or a description (usually)

Scanner Deployment Models

- Stand Alone Single Computer
  - Scanning software installed
  - Scan local computer
- Single Node Network Scan
  - Software or single appliance
  - Scan all connected networks
- Distributed Scanning Architecture
  - Central Management Platform
    - Full Integration with Directory Services Like Active Directory
    - Role based access
  - Central Scan Database
  - Remotely Deployed Scanning Engines
    - Accept scan requests from management node
    - Do the scanning
    - Forward scan results to management node

Distributed Architecture

Parallel scan of multiple networks



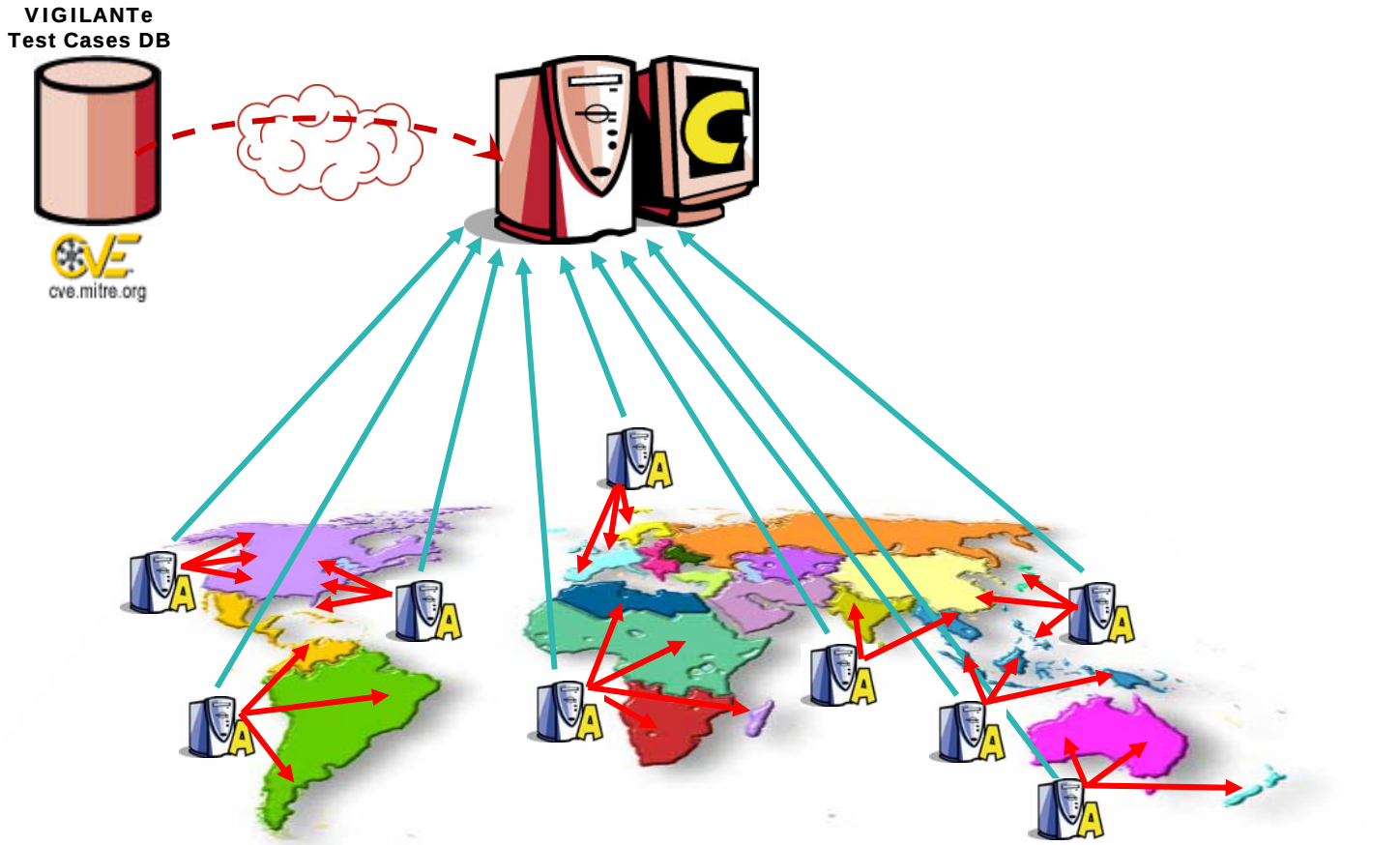
Benefits:

Parallel tasks = Performance

Local view of all network segments

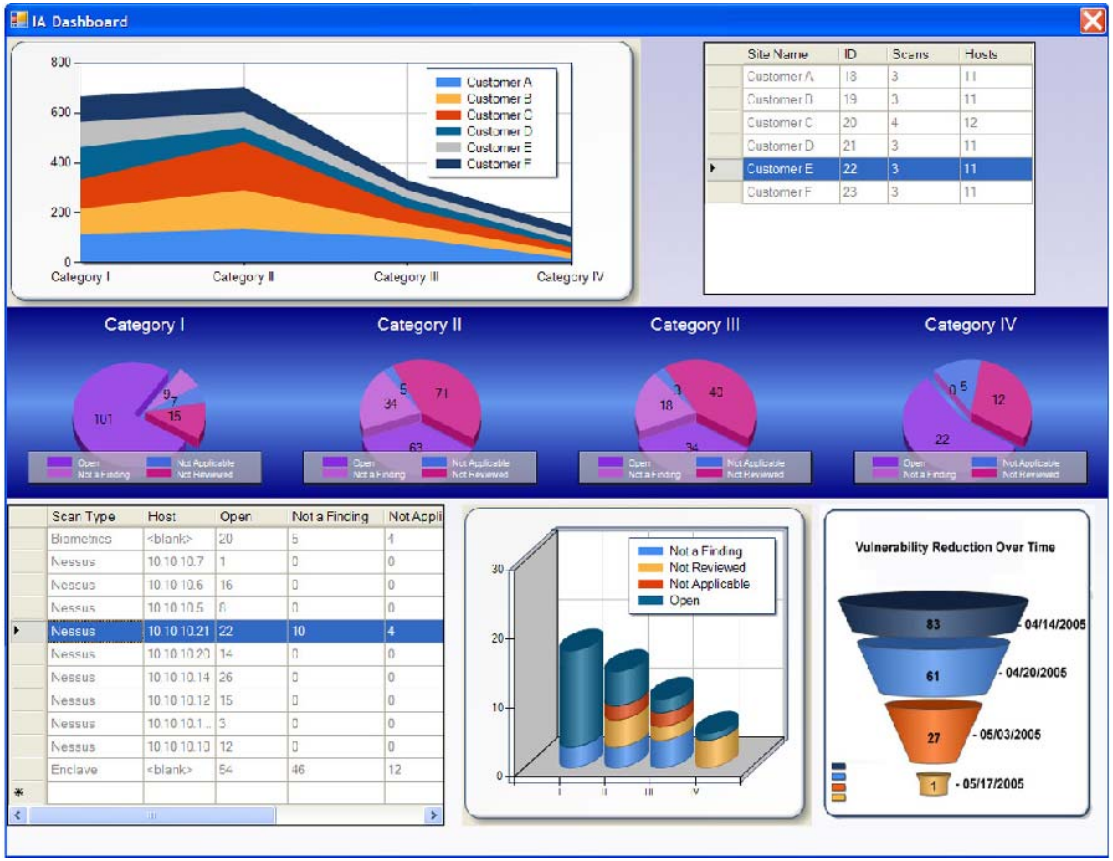
Global report on the entire network

Distributed Architecture



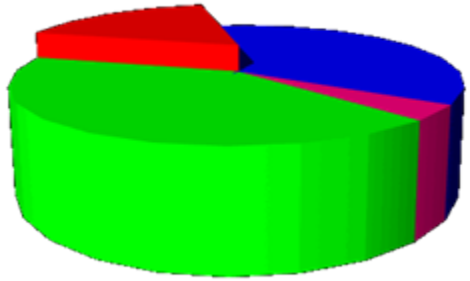
Vulnerability Scanner Output

- High end charts and graphs
- Detailed breakout of vulnerabilities



Selling It to Management

- Small words, big pictures
  - Pictures DO speak louder than words
  - Graphics are more memorable than words
- Business-based graphs
  - OSSTMM RAV-based graphs are ideal
- Be concise
  - Senior management doesn't like marketing fluff
  - Talking too technical can also have a negative effect
- Try to talk in Dollars and Cents
  - Profit and loss amounts can make a big impact
  - Inverse ROI (Return on Investment)
    - www.mcafee.com/us/enterprise/products/tools/ad/roi/index.html
    - www.spamwash.com/roi_calculator.htm
    - www.cleanmessage.com/roi/cost_analysis_virus.asp



Vulnerability Trends

- Less focus on Operating Systems
- More vulnerabilities in:
  - Applications
  - Browsers
  - Web Applications
- More interest in
  - Mobile devices
- Faster discovery of vulnerabilities
- More zero day vulnerabilities

The Future of Vulnerability Scanners

- More integration of general and web vulnerability scanners
- More integration with penetration testing tools
  - Core Impact
    - Import most vulnerability scanner output
    - Launch exploitation attacks against found vulnerabilities
    - True rating of vulnerability risk
- Or… Integrate penetration testing into vulnerability scanner
  - All ready possible to a limited degree in some products

Information Sources

- http://www.wired.com
- http://www.infoworld.com
- http://www.computerworld.com
- http://www.infosecuritymag.com
- http://www.zdnet.com
- http://enterprisesecurity.symantec.com
- http://www.cert.org
- http://www.sans.org

Information Sources

- http://www.fcw.com
- http://www.govtech.com
- http://www.nipc.gov
- http://www.fedcirc.gov
- http://www.ciac.org
- http://www.infosecnews.com
- http://scmagazine.com
- http://www.v-one.com

Kevin Mitnick

- **“People are the weakest link when it comes to security, and an important question to ask yourself is not if, but when, your e-business is going to be targeted."**

Questions???